REMARKS

These remarks are made responsive to the first non-final office action mailed August 20, 2004.

In the drawings, Figure 1 has been amended as indicated on the attached drawing sheet to replace the misspelled "CLINT" with "CLIENT". Furthermore, responsive to the Examiner's paragraph 11, a set of formal drawings, 8 sheets, are submitted herewith including a Drawing Transmittal Letter.

The specification has been amended to add a priority claim as a continuation-in-part to U.S. patent application no. 09/633,077.

An information disclosure statement has also been enclosed herewith along with the fee of $180.00.

Claims 1-3, 5-8, and 13-14 have been amended. Claims 4, 10, and 15 have been cancelled. Claims 9, 11 and 12 remain unamended. Reconsideration of these claims for allowance is respectfully requested in view of the following remarks.

Provisional Non-Statutory Double Patenting Rejection of claims 1-6, 13-15

In his paragraph 2, the Examiner provisionally rejected claims 1-6, 13-15 under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-5, 7-8, 15 of copending application no. 09/704,394.

Since the filing of application no. 09/704,394, the claims of that patent application have been amended including independent claims 1 and 8 of that application. Applicant has submitted with the Information Disclosure Statement submitted herewith a copy of each office action, interview summary and response in that application. The latest response dated October 14, 2004 includes the current state of the claims in that application.

As stated above, in this application, claims 4 and 15 have been cancelled. Claims 1-3, 5-6, and 13-14 have been amended, and claim 9 remains unamended. Claims 1-3, 5-6, 13-14 of this application are patentably distinct over claims 1-5,7-8, 15 of copending application 09/704,394 because claims 1-5, 7-8, 15 include an additional element of an identity authentication module which performs a separate and distinct identity function from a location authentication function performed by the location authentication module

Amendments to the Drawings

In Figure 1, replace “CLINT” with “CLIENT.” A sheet of this drawing indicating this change in red ink is enclosed herewith. Figure 1 in the enclosed set of formal drawings indicates this change.

in claims 1-3, 5-6, 13-14 as amended. The location beacon and location authentication module of claims 1-3, 5-6, 13-14 as amended are directed to verifying that client systems communicating with a web server for a physical entity are close to the physical entity. The identity authentication function of claims 1-5, 7-8, 15 is for authenticating the identity of a user of a client system.

Therefore, claims 1-3, 5-6, 13-14 as amended of this application are patentably distinct from claims 1-5, 7-8, 15 of the co-pending application, and it is respectfully requested that the provisional rejection of claims 1-3, 5-6, 13-14 under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-5, 7-8, 15 of copending application no. 09/704,394 be removed.

Provisional Non-Statutory Double Patenting Rejection of claims 1-15

In his paragraph 3, the Examiner provisionally rejected claims 1-15 under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-14 of copending application no. 09/633,077 in view of Kirsch, U.S. Patent 5,963,915. As discussed above claims 4, 10, and 15 have been cancelled. Claims 1-3, 5-8, 13-14 have been amended. Claims 9, 11-12 remain unamended. Claims 1-3, 5-9, 11-14 as amended of this application are patentably distinct over claims 1-14 of copending application no. 09/633,077 in view of Kirsch, U.S. Patent 5,963,915. Claim 1 as amended of this application from which claims 2-3 and 5-6 depend comprises "a location authentication beacon adjacent to the physical entity and communicatively coupled to the location authentication module for receiving the key and the location token and for generating a customized location token that expires in a predetermined time period and is encrypted using the key and for transmitting a second beacon signal within the predetermined transmission range containing the web address and the customized token." Claim 7 as amended from which claims 8-9 and 11-12 depend comprises "a location authentication beacon adjacent to the physical entity and communicatively coupled to the location authentication module for receiving the key and the location token and for generating a customized location token that expires in a predetermined time period and is encrypted using the key and for transmitting a second beacon signal within the predetermined transmission range containing the web address and the customized token."

Additionally, claim 13 as amended from which claim 14 as amended depends comprises "transmitting a second beacon signal within the predetermined transmission range containing the web address and the customized token from a location authentication beacon adjacent to the physical entity." The versions of a location authentication protocol claimed in these claims is not disclosed, suggested or taught to one of ordinary skill in the art by the combination of claims 1-14 of application no. 09/633,077 in view of Kirsch. One of ordinary skill in the art would not be motivated to combine the claims 1-14 with Kirsch to make the subject matter of claims 1-3, 5-9, 11-14. The specification of 09/633,077 does not disclose the location authentication beacon nor the customized token. Kirsch is not concerned with the client system being close to the physical entity. In fact, its concern is quite the opposite as it deals with the transfer of customer data between multiple vendors so that it appears to the customer that he is purchasing goods from multiple vendors in one transaction over the Internet. (See for example Kirsch 3:41 – 4:51, 9:54-65, 10:47-53). In Kirsch, the transfer of cookies described is after a secure Internet connection has been set-up and the purpose of the cookie transfer is for personal information (See Kirsch 7:55- 8:20) so as to save the customer time from having to enter his data for each separate vendor from which he is purchasing goods in one apparent transaction (See Kirsch 8:64-9:3). Although, encryption is mentioned in Kirsch, there is no disclosure of the protocol in claims 1-3, 5-9, 11-14 of this application. Application no. 09/633,077 is concerned with verifying the location of a client system as being close to the physical entity. One of ordinary skill in the art would not be motivated to combine claims 1-14 with Kirsch to come up with the protocol using a location authentication beacon and a customized token for authenticating whether a client system is close to a physical entity as included in claims 1-3, 5-9, 11-14 of this application. Therefore, claims 1-3, 5-9, 11-14 as amended of this application are patentably distinct from claims 1-14 of the co-pending application 09/633,077, and it is respectfully requested that the provisional rejection of claims 1-3, 5-9, 11-14 under the judicially created doctrine of obviousness type double patenting as being unpatentable over claims 1-14 of copending application no. 09/633,077 be removed.

Rejection of Claim 6 under 35 USC § 112

Claim 6 was rejected for insufficient antecedent basis with respect to the limitation "the random number key." Claim 6 has been amended as indicated to remove the insufficient antecedent basis:

6. (Currently Amended) The ~~web server~~ system of claim 1, wherein the location authentication beacon further comprises

a first token generator that generates the un-encrypted customized token using a stored secret key;

a second token generator that encrypts the customized token using ~~the~~ a random number key ~~into the customized token~~;

a store that stores the customized token and the web address;

a communication interface that receives the web address and the customized token from the store and transmits the second beacon signal.

Rejection of claims 1-4, 13 under 35 U.S.C. 103(a) as being unpatentable over Tracy, 6,199,753, in view of Kirsch, 5,963,915.

Claims 1-3, 13 as amended are patentable over Tracy, 6,199,753, in view of Kirsch, 5,963,915 under 35 U.S.C. 103(a).

Claim 1

Claim 1 as amended for clarity is directed toward a system for a physical entity for authenticating that a user access request to the system is generated from a client system close to the physical entity. The system comprises a web server for providing web content designed for access requests from the client system close to the physical entity. The system further includes a location beacon adjacent to the physical entity to transmit within a predetermined transmission range a first beacon signal containing a web address of the web server and a location token that expires within a predetermined time period.

The system also comprises a location authentication module for authenticating that the client system having received the first beacon signal is still close to the physical entity wherein the location authentication module receives a first request including the web address, the location token, and the key from the client system._ The location authentication module forwards the key to a location authentication beacon adjacent to the physical entity for encrypting a customized location token using a key, the customized location token expiring in a predetermined time period. The location authentication beacon transmits a second beacon signal containing the web address and the customized token within the predetermined transmission range. Responsive to receiving a second request from the client system including the web address of the web server and the customized token, and it being unexpired, the location authentication module causes the web server to provide web content designed for an access request from the client system close to the physical entity.

Neither Tracy nor Kirsch alone or in combination disclose nor suggest any system for determining whether a client system is close to the physical entity. In Tracy, a customer inserts a magnetic card identifying the customer to the centralized system in order to activate a dispenser unit to assign a portable terminal to the customer. Before the portable terminal leaves the dispenser unit and is in the hand of a customer, the server in the store or the server network located outside the store has linked the customer to that terminal, has that customer's data file and the IP address of that terminal. Additionally, before the terminal leaves the dispenser unit, the terminal has the web address of the server. (See Tracy, Figure 9 and columns 6:66 to 7:61.) There is no discussion or suggestion of how the supermarket system tracks the location of a client system within the store, perhaps, because there is no need for transmission of a web address of the server to terminals that already have the web address stored. Kirsch provides no suggestion that location is a factor at all. It provides encryption of confidential information, not for the purpose of verifying that a client system is close to a physical entity. As mentioned above, Kirsch is concerned with a user only having to provide his personal information once in making purchases from multiple vendors over an Internet connection in one transaction. Both Tracy and Kirsch mention that confidential data can be encrypted for protecting client data, but not for customizing location tokens as part of a system for authenticating that a client system is close to a physical entity.

Furthermore, the combination of Tracy in view of Kirsch fails to suggest or motivate one of ordinary skill in the art that an electronic coupon is a location token as that term is used in claim 1. Coupons do not necessarily have expiration times, but even for those that do, the combination of Tracy in view of Kirsch fails to suggest, teach or provide motivation that an expiration period of an electronic coupon unlike the expiration of a predetermined time period for a location token that a client system is close to the physical entity. Tracy specifically illustrates that the coupons are not an indicator of location of a client device as customers can scan coupons using a home scanner attached to their home computers and download the data into their customer data files at the store (See 13:11-14). Kirsch does not describe at all a location basis for communication of content. In fact, processing purchases from multiple vendors is more of a motivation for making completion of access requests and the content provided independent of the location of a client system proximate to a physical entity. In Kirsch and Tracy, encryption is referenced for keeping customer information confidential but not for encrypting location tokens to authenticate the location of a client system. Encrypting electronic coupons having expiration dates and sending them back to a central server does not server the purpose of location authentication. Claim 1 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch.

Claim 2

Claim 2 depends from claim 1. The arguments with respect to claim 1 are also applicable to claim 2. Furthermore, the combination of Tracy in view of Kirsch fails to disclose teach, suggest to or motivate one of ordinary skill in the art to make "the system of claim 1, wherein responsive to the location token in the first request being expired, the location authentication module causes the web server to provide content designed for an access request from a client system not close to the physical entity." Tracy does not distinguish between content designed for an access request from a client system within the store and that from a client system not close to the store. Kirsch is not concerned with location at all much less encryption of location tokens have predetermined time periods, the expiration of which are a basis for directing content dependent on the proximity of a client system to a physical entity. Therefore, the combination of Tracy in view of Kirsch does not motivate one of ordinary skill in the art to make the subject matter of claim 2. Claim 2 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch.

Claim 3

Claim 3 is unamended and depends from claim 1 as amended. The arguments with respect to claim 1 are also applicable to claim 3. Furthermore, coupons do not always have expiration dates so coupons do not by definition expire. Claim 3 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch.

Claim 4

Claim 4 has been cancelled.

Claim 13

Claim 13 is patentably distinct under 35 U.S.C. 103(a) over Tracy in view of Kirsch. As discussed above with respect to claim 1, this combination fails to disclose, teach, suggest to or motivate one of ordinary skill in the art to devise a method of authenticating the location of a client system accessing a web server system associated with a physical entity. As mentioned above Tracy does not address the authentication of location as the portable terminal is assigned to a customer, linked with the customer's data file, and the IP addresses of the terminal and web server are stored within the terminal and the web server prior to release of the terminal from the dispenser unit to the customer's hands. As discussed above, Kirsch is not concerned with the location of a client system, and refers to encryption generally for protection of a client's confidential information and not to a specific set of actions, as described in claim 13, for authenticating the location of a client system with respect to a physical entity based on a customized token. Therefore, this combination fails to motivate one of ordinary skill in the art to perform or devise at least transmitting within a predetermined transmission range a first beacon signal containing a web address of the web server system and a location token that expires within a predetermined time period from a location beacon adjacent to the physical entity. Also, specifically not taught nor suggested by the combination is generating a random number key in the client system close to the physical entity. Claim 13 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch.

Claims 5-15 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tracy, U.S. Patent No. 6,199,753, in view of Kirsch, U.S. Patent No. 5,963,915, as applied to claim 1 above, and further in view of Schneier.

Claim 5

Claim 5 depends from claim 1. The arguments presented with respect to claim 1 are also applicable to claim 5. Therefore, claim 5 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above, and further in view of Schneier.

Claim 6

Claim 6 depends from claim 1. The arguments presented with respect to claim 1 are also applicable to claim 6. Furthermore, none of the elements which the location authentication beacon further comprises are disclosed or suggested by the combination of Tracy, in view of Kirsch as applied to claim 1 above, and further in view of Schneier. One of ordinary skill in the art would not be motivated by the description of the dispensing of the terminals in Tracy and the brief references that confidential customer information should be encrypted in Tracy and Kirsch to make a *location authentication beacon* comprising the elements of claim 6 such as a first token generator, a second token generator, a store that stores the customized token and the web address, and a communication interface as claimed. Therefore, claim 6 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above, and further in view of Schneier.

Claim 7

Claim 7 as amended is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above, and further in view of Schneier.

As discussed above with respect to claim 1, this combination fails to disclose, teach, suggest to or motivate one of ordinary skill in the art to make a system for authenticating the location of a client system accessing a web server system associated with a physical entity. As mentioned above Tracy does not address the authentication of location as the portable terminal is assigned to a customer, linked with the customer's data file, and the IP addresses of the terminal and web server are stored within the terminal and the web server prior to release of the terminal from the dispenser unit to the customer's hands. As discussed above, Kirsch is not concerned with the location of a client system, and refers to encryption generally for protection of a client's confidential information and not to a specific set of structures, as described in claim 7, for authenticating the location of a client system accessing a web server system associated with a physical entity based upon a customized token. Therefore, this combination fails to motivate one of ordinary skill in the art to make a system for authenticating the location of a client system accessing a web server system for a physical entity comprising any of the elements of claim 7, one example of which is a location beacon adjacent to the physical entity to transmit within a predetermined transmission range a first beacon signal containing a web address of the web server system and a location token that expires within a predetermined time period.

Also another example of an element not taught nor suggested by the combination to one of ordinary skill in the art is a location authentication module for authenticating that the client system having received the first beacon signal is still close to the physical entity wherein the location authentication module receives a first request including the web address, the location token, and the key from the client system, and that causes the web server to provide content designed for an access request from the client system close to the physical entity responsive to receiving a second request from the client system including the customized token and the web address. Therefore claim 7 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above and further in view of Schneier.

Claim 8

Claim 8 depends from claim 7. The arguments with respect to claim 7 are also applicable to claim 8. Furthermore, claim 8 as amended is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above and further in view of Schneier as this combination fails to disclose, teach, suggest to or motivate one of ordinary skill in the art to make "the system of claim 7, wherein responsive to the location token in the first request being expired, the location authentication module causes the web server to provide web content designed for an access request from a client system not close to the physical entity." Tracy does not distinguish between content designed for an access request from a client system within the store and that from a client system not close to the store. Kirsch is not concerned with location at all, much less encryption of a customized token having predetermined time period whose expiration indicates the proximity of a client device to a physical entity. Schneier's reference to random number generation does not provide the necessary motivation or suggestion for a location authentication system lacking in the other two to the combination. Therefore claim 8 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above and further in view of Schneier.

Claim 9

Claim 9 is unamended and depends from claim 7 as amended. The arguments with respect to claim 7 are also applicable to claim 9. Furthermore, coupons do not always have expiration dates so coupons do not by definition expire. Therefore claim 9 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above and further in view of Schneier.

Claim 10

Claim 10 has been cancelled.

Claim 11

Claim 11 is unamended and depends from claim 7 as amended. The arguments with respect to claim 7 are also applicable to claim 11. Furthermore, none of these references suggest a beacon receiver, much less any of the elements it comprises as recited in claim 11. Therefore claim 11 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above and further in view of Schneier.

Claim 12

Claim 12 is unamended and depends from claim 7 as amended. The arguments presented with respect to claim 7 are also applicable to claim 12. Furthermore, none of the elements which the location authentication beacon further comprises are disclosed or suggested by the combination of Tracy, in view of Kirsch as applied to claim 1 above, and further in view of Schneier. One of ordinary skill in the art would not be motivated by the description of the dispensing of the terminals in Tracy and the brief references that confidential customer information should be encrypted in Tracy and Kirsch to make a *location authentication beacon* comprising the elements of claim 6 such as a first token generator, a second token generator, a store that stores the customized token and the web address, and a communication interface as claimed. Therefore, claim 12 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 7 above, and further in view of Schneier.

Claim 13

As explained above, claim 13 as amended is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch. Furthermore, the addition of the reference to random number generation in Schneier fails to provide the motivation or suggestion to one of ordinary skill in the art to devise any of the elements of the method of claim 13. Therefore, claim 13 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above, and further in view of Schneier.

Claim 14

Claim 14 as amended depends from claim 13. The arguments presented above for claim 13 are also applicable to claim 14. Furthermore, Tracy does not distinguish between content designed for an access request from a client system close to the store and that from a client system not close to the store. Kirsch is not concerned with location at all, much less directing content dependent on the proximity of a client terminal to a physical entity based on an expiration of a predetermined time period of an encrypted customized token. Schneier's reference to random number generation does not provide the necessary motivation or suggestion for providing content based on whether a client system is close to a physical entity or not lacking in the other two to the combination. Therefore claim 14 is patentable under 35 U.S.C. 103(a) over Tracy in view of Kirsch as applied to claim 1 above and further in view of Schneier.

Claim 15

Claim 15 has been cancelled.

Information Disclosure Statement References

The additional references cited in the information disclosure statement do not disclose the subject matter of claims 1-3, 5-9, and 11-15 of the current application as whether a client system is close to the physical entity is not relevant to the disclosures of these additional references. Furthermore, the references in any combinations do not suggest or teach or motivate one of ordinary skill in the art to make the subject matter of claims 1-3, 5-9 and 11-15.

Conclusion

In light of the arguments presented above, pending claims 1-3, 5-9 and 11-15 as amended are in condition for allowance, and applicants respectfully request a prompt notice of allowance.

Date: 12/20/04

Respectfully Submitted on Behalf of Applicants
Deborah L. Caswell, et al

Eileen Lehmann

Eileen Lehmann
Registration No. 39,272
Hewlett-Packard Company
Mail Stop 1197
1501 Page Mill Road
Palo Alto, CA 94304
650-857-7940 (telephone)
650-852-8063 (fax)

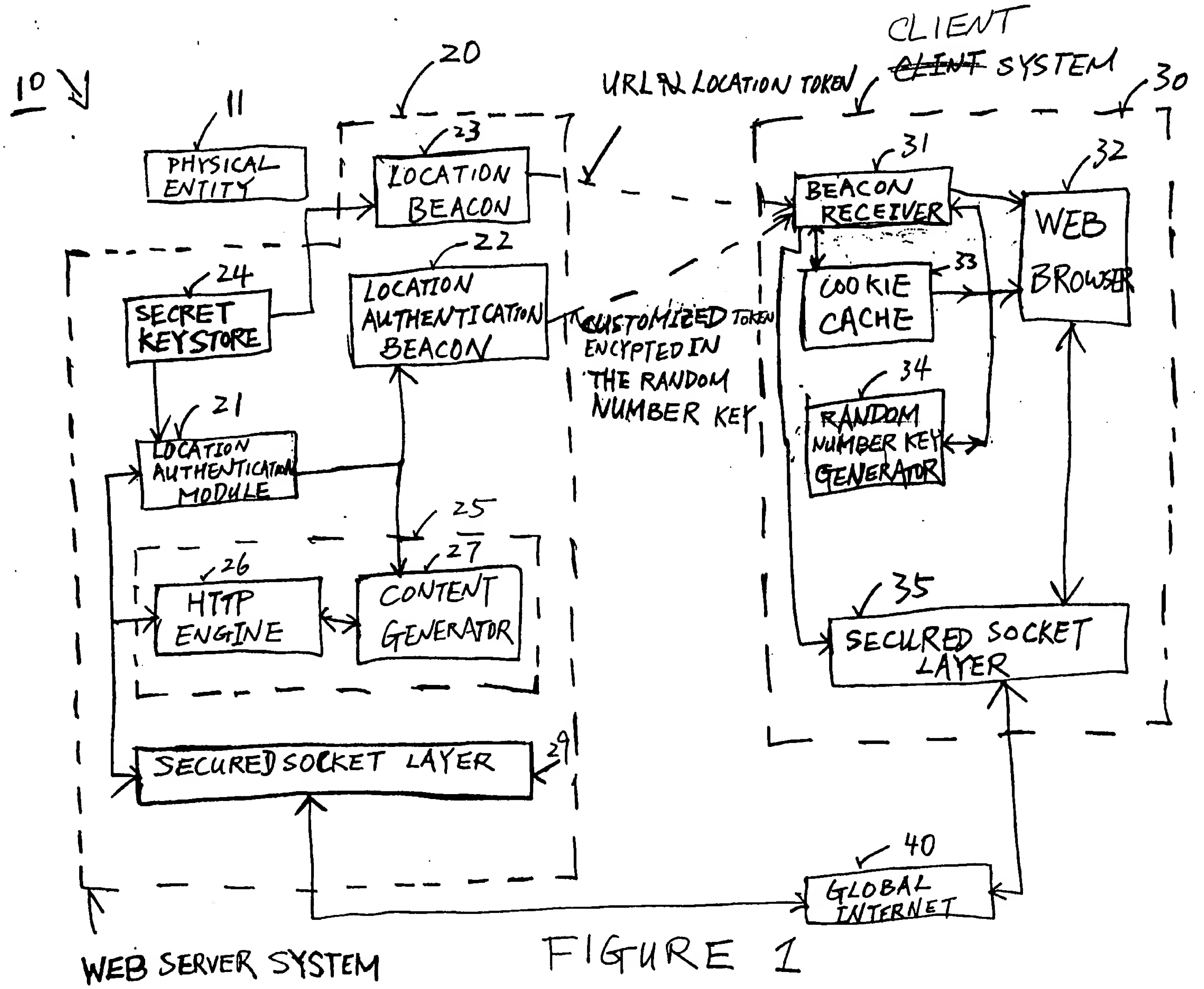
10
11
PHYSICAL ENTITY
20
23
LOCATION BEACON
22
LOCATION AUTHENTICATION BEACON
24
SECRET KEYSTORE
21
LOCATION AUTHENTICATION MODULE
25
26
HTTP ENGINE
27
CONTENT GENERATOR
SECURED SOCKET LAYER
29
WEB SERVER SYSTEM
URL ~~N~~ LOCATION TOKEN
~~CUSTOMIZED~~ CUSTOMIZED TOKEN ENCYPTED IN THE RANDOM NUMBER KEY
CLIENT ~~CLINT~~ SYSTEM
30
31
BEACON RECEIVER
32
WEB BROWSER
33
COOKIE CACHE
34
RANDOM NUMBER KEY GENERATOR
35
SECURED SOCKET LAYER
40
GLOBAL INTERNET

FIGURE 1